POLICY 1460.00

Issued Date: July 31, 2003
Effective Date: September 1, 2003

IT Resources Acceptable Use Policy
Acceptable Use Agreement Acknowledgement

1.0 Purpose: This policy identifies acceptable use of State of Michigan Information Technology Resources, provides awareness of expected end-user behavior, and is also intended to safeguard IT data resources. This policy requires that end-users maintain respect for the privacy of protected citizen and employee information at all times. A cooperative effort from every employee is necessary to prevent misuse, eliminate the risk of liability to the State, and promote the efficient utilization of IT resources and information technology services.

2.0 Revision History:

Date	*Revision Number*	*Change*	*Reference Section*
31 Jul 03	00		

3.0 Persons, Groups, & Systems Affected:

3.1 All executive branch agency computer end-users; including employees, interns, vendors, contractors, and volunteers.
3.2 State hosted application specific end-user-agents at county and local units of government.
3.3 System and network administrators.
3.4 Lead-workers, supervisors, administrators, and managers at all levels.
3.5 DIT Office of Enterprise Security (OES).
3.6 All computing equipment, devices, systems, servers, and data networks.

4.0 Policy:

4.1 A primary mission of the Department of Information Technology (DIT) is to provide and support end-user computing devices, systems, applications, and network communications resources. These resources are for the official use by executive branch employees to meet the daily operational and business requirements of departments, agencies, and the various boards and commissions of the State of Michigan. Information technology resources provided to employees are for the purpose of delivering public services to the State's diverse groups of customers in a more efficient manner. Employees should have no expectations of personal privacy protection when using State owned IT resources.

4.2 Acceptable uses of IT resources include:

A. Uses authorized by agency business units, with the exception of items listed in section 4.3.
B. Personal use by employees for interaction with human resource, time accounting, compensation, and employee benefits and health administration programs managed by or administered for the State of Michigan.
C. Access to information and transactions made available on the e-Michigan portals.

D. Use of applications or access to information provided for general audience use on enterprise or agency intranet hosts.

E. Access to Internet hosted on-line reference and information sources such as phone directories, on line dictionaries, or mapping and weather services if such use adds value to the business unit, increases employee efficiency, or legally avoids costs that would otherwise be incurred by the State of Michigan for such referenced services.

F. Statutory and regulatory activities.

4.3 Unacceptable uses of IT resources include (but are not limited to):

A. Any use of computer equipment that violates State or U.S. law and regulations are clear violations of acceptable use. The deployment, delivery, and use of technology resources within State of Michigan executive branch agencies is governed by statute and published procedures such as those contained in the DMB administrative guide or within specific department and work group policies. Computer end-users and their direct supervisors must be aware of and be accountable for the elements of these laws, regulations, policies, and procedures as they affect daily work and responsibilities related to the use of IT resources utilized within their line of business work group.

B. Creating or forwarding of chain mail regardless of content, sources, or destinations. Posting agency information to external newsgroups, bulletin boards or other public forums without authority.

C. Using equipment for personal profit, political fundraising, gambling activity, non-business related instant messaging or chat room discussions, and downloading or display of offensive material.

D. Any use that violates public safety or compromises the privacy of legally protected resident or citizen information.

E. Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.

F. Use of any remote control software on any internal or external host personal computers or systems not specifically set up by DIT staff using methods authorized by standard or policy.

4.4 All employees or computer end users shall be made aware of this policy and educated about its content and the impact of violations of acceptable use criteria.

A. Awareness and education:

(1) Each executive branch end user is required to acknowledge this policy.

(2) Log in screen reminders (appendix 1) are required for periodically reminding employees of this and similar policies directly affecting end-users. These reminders will be presented on screen prior to or during the logging in routine.

(3) IT training sponsored by the State of Michigan may include a segment on this policy and good cyber-citizenship.

(4) Application specific security rules and procedures mandated by State of Michigan and federal regulations must also be rigorously adhered to in order to safeguard legally protected data resources from compromise and should be a part of agency sponsored privacy and security awareness efforts.

(5) Every user should perform due-diligence measures to contribute to a professional, safe, pleasant, and non-offensive IT user environment. Remember: e-mail is subject to the Freedom of Information Act (FOIA). E-mail and other information may still remain on your PC after deletion.

(6) Violation of this policy may result in agency-administered discipline up to an including discharge. Criminal or civil action may be initiated in appropriate instances.

B. Inadvertent and Erroneous use – End-users inadvertently directed to a web site that violates laws, regulations, or polices may claim erroneous use. Mistakes occur when using IT resources without any employee intent to violate policy. A claim of this type is only substantiated by connection times measured in seconds, rather than minutes when found in network, system, or application log audits done to verify or detect abuse. Report to supervisors or managers when un-intentional misuse occurs. Self-reporting is encouraged and may be done without consequence.

5.0 Definitions:

Agency- means executive branch entities including agency, department, board, or commission.

AIO – Agency Information Officer

Business Units - Supervised areas of related work responsibility as explicitly defined and delegated to them by executive branch agency directors, boards, or commissions of the State of Michigan.

Chain Mail- unauthorized non-government or NON-business related e-mail to large groups, the SOM address book, or to unspecific destination addresses that suggest that the receiver should further disseminate the message.

DMB – Department of Management & Budget

Due Diligence - activities that ensure the protection mechanisms are continually maintained, operational and applicable to state and federal laws.

Employees or computer end-users - includes the broad range of persons who are supplied with any IT resources or application access by DIT to accomplish State work and include all executive branch agency employees; including interns, vendors, contractors, volunteers, and agents at county and local units of government who are given password access to specific State of Michigan hosted applications.

Hacking -- Gaining or trying to gain unauthorized access to systems and databases either internal or external to the State of Michigan computer systems or networks for the purpose of viewing, stealing, or corrupting data.

IT systems or resources -- Data networks (over any media type); computer devices including: servers, hosts, laptops, desktops, handheld, or tablet pc; communication devices: phone, web phones, or pagers; and software applications accessed with any interface device.

Mass Mail- authorized State of Michigan business related e-mail to large groups or the whole SOM address book sponsored or originated within an agency business unit.

OHR – Agency Office of Human Resources

OES – DIT Office of Enterprise Security

OUs (operations units) -- describe any employee groups of DIT functions supporting specific agencies and/or applications.

SOM -- State of Michigan

6.0 Responsibilities:

6.1 Employee end-users -- must read this document, understand the expectations and take personal responsibility for adhering to the provisions of this policy. Each end-user will be required to acknowledge receipt of this policy and any agency specific addendums. All categories of employees must realize that misuse or abuse of IT resources may lead to department or agency investigation and initiation of legal or disciplinary actions. Be aware that computers assigned to you may also be removed from your office area for analysis.
6.2 Agents, contract staff, vendors, and volunteers – are required to adhere to this policy, acknowledge an awareness of this policy, however realizing the consequences of willful violation will be appropriate to their status.
6.3 Supervisors, managers, or directors -- make up the first line of accountability for staff compliance with this policy and shall require that all staff under their management read, and acknowledge the acceptable use agreement, and abide by the provisions of this policy
6.4 Agency OHR – shall support supervisors and managers as needed in the awareness and disciplinary enforcement of this policy.
6.5 DIT staff and OUs– shall report suspected violations to OES when found in the normal course of system support activity and assist OES with audits and enforcement actions when requested to do so.
6.6 Office of Enterprise Security (OES) -- shall receive and document reports of suspected abuse from any source and act as necessary on each reports. OES shall plan and supervise periodic system and network audits to detect potential abuse and shall use these audits to identify and investigate non-compliance with the provisions of this policy. Report incidents of abuse to agency DIT AIO, agency OHR liaison, and agency internal auditor, and where abuse may involve criminal activity to appropriate State of Michigan or other law enforcement officials. Assist in the collection and preservation of digital forensic evidence when requested by law enforcement officials.
6.7 Agency Business Units - shall ensure that all aspects of the IT Acceptable Use policy and standards are communicated to staff within their divisions and work groups.
6.8 Contracts Management and Purchasing Division – Holds the responsibility to communicate acceptable use policy to vendors and contract staff that will be using IT resources, emphasizing the need for ensuring compliance with this policy. Purchasing process shall include contract language requiring vendors' staff to follow acceptable use policies, and require that all vendor staff acknowledge the acceptable use agreement.

7.0 Procedures:

The policy described in this section sets a minimum level of conformance that will be implemented across the State of Michigan enterprise. Agency work rules should support this policy direction and provide departmental guidance on how violations will be handled. Work rules or policies that are consistent need not be reissued. State Departments desiring to implement more restricitve policies regarding information technology resources may do so by coordinating with OEM prior to implementation.

This policy replaces policy 1310.16.

Authority is The Management and Budget Act, Public Act 431 of 1984, as amended, § 203.

* * *

Appendix 1

Sample Screen Acceptable Use Agreement login acknowledgement in Window or Banner:

I have read and am fully aware of the

STATE OF MICHIGAN

Information Technology
Resources
Acceptable Use Policy

# 1460.00

I understand that I am expected to

act in accordance **with this policy**

when using State of Michigan computing equipment and applications at all times.

Full Policy Available at: **Michigan.gov/pcpolicy**

* Please note, ideally the on screen AUA banner should include a link to the complete policy document.